UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/770,525	01/25/2001	Michael Hrabik	881075/3	5856

7590 12/26/2002

Joel E. Lutzker, Esq.
SCHULTE ROTH & ZABEL LLP
919 Third Avenue
New York, NY 10022

EXAMINER
JACKSON, JENISE E

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 12/26/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

7

Office Action Summary	**Application No.** 09/770,525	**Applicant(s)** HRABIK ET AL.	
	Examiner Jenise E Jackson	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 August 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: .

Minor Informalities

1. Figure 1 is prior art; it should be labeled as such.

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: reference number 50 is not found in the drawing Figure 2. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

3. The Applicant states on page 6, "that fig. 2, a first embodiment of the present invention is shown. Target network(100) is shown having the same basis components as the network of the prior art shown in fig. 1". However, the Examiner asserts that figure 2 is not the same as fig. 1. Figure 2, is missing reference signs 14, 12, 22, 24, 26.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 3-7, 9-11, 13-15, and 17-19, 21-22 are still rejected under 35 U.S.C. 103(a) as being unpatentable over Emigh in view of (Violino and Netwon Telecom Dictionary).

6. As per claim 1, Emigh teaches that IBM has a new hacking prevention service that combines onsite, real-time intrusion detection through NetRanger sensors. NetRanger intrusion detection sensors are located at places on a corporate network. Thus, the Examiner asserts that by having intrusion detection sensors on the corporate network, this constitutes a security

subsystem, because if the security subsystem detects intrusion or misuse, the Network Security Operations Center(NSOC) is contacted. Therefore, Emigh teaches that there is at least one security subsystem associated with the computer, and that the subsystem is configured to detect attacks on the computer. Also, because the applicant provides no specific definition of a master system, the Examiner broadly interprets a master system to be any system that is in control over another system/subsystem, thus Emigh teaches a master system(i.e. NSOC) that monitors the security subsystem, because all intrusion or misuse that is detected by the security subsystem is sent in real-time to the NSOC in Colorado. Furthermore, NSOC registers information pertaining to attacks, because Emigh teaches that NSOC regularly issue written reports to customers as to the security status of their customers networks, and IBM consolidates NetRanger director log files from multiple customers into a separate database for trend analysis to uncover patterns in detected activities of hackers. Emigh discloses intrusion sensors located at places on a corporate network such as Internet and intranet connections(pg. 1). The Examiner asserts that one sensor can be located on the Internet connection, and this constitutes the security subsystem. The Examiner takes Official Notice that monitoring at these "connections" result in monitoring the network in its entirety, motivation is that that by monitoring at these connections would result in all intrusion information being routed to these connections and then routed to NSOC(i.e. Master system).

7. Although, Emigh teaches that the security subsystem and a master system(i.e. NSOC) have communication, because when the security subsystem detects a misuse it communicates by sending an alarm to NSOC. Emigh does not explicitly disclose what link is used in order to communicate between the security subsystem and the master system. However, Violino teaches

that Netranger security management system uses an encrypted communication channel(i.e. secure link, pg. 2). According to Newton's Telecom Dictionary, a secure channel is defined as technology that provides privacy, integrity, and authentication in point-to-point communication. Thus, the Examiner asserts that the encrypted channel is a secure channel(i.e. link), because encrypting insures that information is protected form unauthorized viewing or use; therefore insuring privacy, and integrity is maintained because if information is private the information cannot be manipulated, and authentication because in encryption in order to decode the information one must have the key. Thus, the motivation to have an encrypted channel(i.e. secure link) is that information that is sent between to points such as in Emigh between a master system and a security subsystem is that information is kept private, integrity is kept, and parties can be authenticated, and thus prevents intruders or unauthorized users from manipulating information.

8. Claims 2, 8, 16, 20, are still rejected under 35 U.S.C. 103(a) as being unpatentable over Emigh in view of (Violino and Newton Telecom Dictionary), in view of Kurtzberg et al. and further in view of Hill et al.

9. As per the claims above, Emigh teaches that NSOC test network devices for vulnerability. However, Emigh is silent on how NSOC test for vulnerabilities. However, Kurtzberg et al. discloses testing a system by having a pseudo(i.e. simulated) attack generator for generating attacks on the computer(see col. 3, lines 21-28). Although, Emigh does not explicitly disclose comparing pseudo-attacks to the attacks detected by the security system, the Examiner looks towards Hill et al. for this feature. Hill et al. discloses comparing pseudo-attacks(i.e. training attacks) to the attacks detected by the security system(see col. 3, lines 20-36).

10. It would have been obvious to modify Emigh and the teachings of (Violino and Newton), with the features of Kurtzberg et al. and Hill et al. The Emigh-(Violino and Newton Dictionary), combination, teach testing for vulnerabilities; however, do not teach how the testing is done. Therefore, the Examiner looks towards Kurtzberg et al. and Hill et al. to include the features of pseudo attack generator and comparing the pseudo attacks to attacks detected by the system. Thus, the motivation to include how the testing is performed of Kurtzberg and Hill et al. with the Emigh-(Violino and Newton), combination includes NSOC testing for vulnerabilities of the security subsystem by using the pseudo attack generator, and comparing the pseudo attacks to attacks detected by the system. This method of testing, insures that integrity is maintained by testing the security subsystem thereby protecting the network from unauthorized penetrations (see col. 1, lines 35-40 of Kurtzberg et al.). Thus, integrity of a computer system can be tested reliably to improve or complement the system performance(see col. 1, lines 65-67 of Kurtzberg).

11. As per claim 3, Emigh teaches that the master system(i.e. NSOC) is hierarchically independent from the security subsystem; because when intrusion or misuse is detected an alarm is sent to NSOC(i.e. master system), which is located in Colorado. Thus, the master system is independent from the security subsystem.

12. As per claim 4, Emigh teaches that a security subsystem is hierarchically subordinate to the master system, because Emigh discloses that the customer's that are on the corporate network that have NetRanger intrusion detection sensors located at places on the network have an intrusion or misuse, the NSOC(i.e. master system) is contacted, thus the Examiner asserts that the security subsystem does not handle intrusion detection, all misuse or intrusion detection is

sent to the NSOC. Therefore, the Examiner asserts that the security subsystem is subordinate to the master system(i.e. NSOC).

13. As per claim 12, rejected under the same basis as claim 1, and further, generating a list of expected responses to at least one pseudo-attack(see col. 1, lines 65-67, and col. 3, lines 1-20).

14. As per claim 13, rejected under the same basis as claim 1, and further, Emigh teaches at least one detection means, because Emigh teaches NetRanger intrusion sensors associated with the computer, and NetRanger sensors are configured to detect an attack on the computer.

15. As per claim 14, Emigh teaches the detection means(i.e. NetRanger) is one or more selected from the group consisting of an intrusion detection system, a firewall and a security subsystem, the Examiner asserts that Emigh meets this limitation, because NetRanger intrusion detection sensors is an intrusion detection system, that detects misuse or intrusions on the network.

16. As per claims 5 and 11, rejected under the same basis as claim 1, and further, the target network is the corporate network of Emigh.

17. As per claim 17 and 21, rejected under the same basis as claim 13.

18. As per claims 6, 9, 15, 19, rejected under the same basis as claim 3.

19. As per claims 7 and 10 rejected under the same basis as claim 4.

20. As per claim 18, rejected under the same basis as claim 14.

21. As per claim 22, rejected under the same basis as claims 1 and 3.

Cited But Not Applied

22. PC Week, IBM Making E-commerce Safer, More Reliable

23. Giles, Internet Security

24. Rutrell, Managed Security Gets Sophisticated

25. Electronic Commerce News, and Yasin Managed Security Gets Sophisticated

26. Messmer, Cultivating Managed Security Outsourced Security Can Ease Admin.

27. Higgins, Call In The Guards: More Companies Seek Outside Security

28. E-Commerce Sites Under Heavy Attack From Hackers

29. Shipley, Enterprise-Class ISPs: The Big Eight Revealed

30. US 5,796,942, Method for Automated Network-Wide Surveillance and Security Breach Intervention

31. US 5,909,493, Method and System For Diagnosis And Control Of Machines Using Connectionless Modes Of Communication

Response To Amendment

32. The Applicant has submitted a response 10/2/02, the Applicant's argument is considered moot, for the following reasons:

33. The Applicant states that the present invention relates to a method and apparatus for monitoring the integrity and security of a computer network. The Applicant states that the security of the present invention monitors the integrity of an individual computer connected to a target network and/or the entire target network by having at least one security subsystem.

34. The Applicant's argument is stated on page 7 of paper 11, the Applicant states that NetRanger product passively captures information from devices associated with them on a computer network. The Applicant points out in the specification that network IDS(18) shown in fig. 1, is like the NetRanger is monitoring a limited area of the network from a fixed point of

view. The Applicant is showing the IDS(18) and says it is the same as NetRanger sensor, because it only monitors a fixed point, not the entire network. The Examiner has taken the argument in consideration with regards to the new limitation that was added, and asserts that Emigh still on this added feature.

35. Secondly, the Applicant states that as disclosed in the Electronic Commerce News reference, that NetRanger sensors are deployed at critical locations on a company's network. Further, the Applicant states that deployment of multiple sensors in several fixed locations is necessary for devices based on the intrusion detection technology because of their limited event view. The Examiner agrees with the Applicant in regards to the feature of sensors being individually deployed at critical locations on a company's network. However, Emigh also teaches that sensors located on Intranet and Internet connections.

36. Thirdly, Emigh reference does not explicitly teach a security subsystem(i.e. Network sensor) that is configured to monitor events across the ***network of computers in its entirety***. Although, Emigh teaches that the sensor look into the data stream, analyzing it for signatures of misuse. Emigh teaches that the sensors are located on multiple places on the network, and the sensor can be located on Intranet and Internet connections, thus the sensor is monitoring the all data streams that come into the network.

37. The Examiner acknowledges and considered publication patent application US2001/0034847A1.

Action Final, Necessitated By Amendment

38. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (703) 306-0426. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes can be reached on (703) 305-9711. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-0040 for regular communications and (703) 308-6306 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

***
December 11, 2002

Gail Hayes

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100